

УТВОРИ

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)



УТВЕРЖДАЮ

Проректор
по образовательной деятельности

А.А.Панфилов

« 29 » 12 2016 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ
(наименование дисциплины)

Специальность 10.05.04 "Информационно-аналитические системы безопасности"

Специализация "Автоматизация информационно-аналитической деятельности"

Уровень высшего образования специалитет

Форма обучения очная

Семестр	Трудоемкость зач. ед./ час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
5	4/144	36	18	36	18	Экзамен (36ч), КР
Итого	4/144	36	18	36	18	Экзамен (36ч), КР

Владимир 2016

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Криптографические методы защиты информации» являются обеспечение подготовки бакалавров в соответствии с требованиями ФГОС ВО и учебного плана по специальности 10.05.04 «Информационно-аналитические системы безопасности», ознакомление студентов с основами теории двоичного кодирования, алгоритмами сжатия, помехоустойчивого кодирования. Дисциплина «Криптографические методы в защите информации» рассматривается как теоретическая и прикладная дисциплина, дающая представления об основных математических и алгоритмических подходах, применяемых для хранения, передачи, исправления информации, представленной в двоичных кодах. Дисциплина посвящена изучению основ криптографии и криптографического анализа, применяемых к защите информации в информационных системах. Обучаемые знакомятся с понятием шифров, симметричной и асимметричной криптографии, электронной подписью, хешированием и другими математическими объектами криптографии. Изучаются соответствующие криптографические стандарты, применяемые сегодня в защите информации в России и за рубежом. Подробно рассматриваются: стандарты RSA, DES, GOST1989, и другие. Также уделено внимание перспективным направлениям в криптографии: криптографические протоколы с разглашением и без разглашения, теория алгоритмической сложности и односторонних функций, схемы разделения секрета и некоторые их приложения в задачах идентификации и аутентификации.

Задачами изучения дисциплины «Криптографические методы в защите информации» являются: -ознакомление с основами математической теории криптологии; - приобретение навыков в практическом использовании, постановке и решении задач шифрования информации; - понимание сути информационных процессов в криптографических системах; - применение компьютеров для решения задач шифрования и дешифрования; - разработка и использование математических и вычислительных моделей процессов шифрования информации, их оптимизация и выработка направлений совершенствования.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО СПЕЦИАЛИТЕТА

Данная дисциплина относится к базовой части Блока Б1 (код Б1.Б.10). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций, лабораторных работ и практических занятий.

Дисциплина изучается на 3 курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по курсам «Математика», «Информатика» по специальности 10.05.04 «Информационно-аналитические системы безопасности», квалификации - специалист. Курс тесно взаимосвязан с другими дисциплинами данного цикла. Он является полезным для изучения таких дисциплин как «Основы информационной безопасности», «Техническая защита информации», «Программно-аппаратные средства защиты информации», «Математические методы в информационной безопасности».

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины бакалавр должен обладать следующими общепрофессиональными компетенциями:

ОПК-7 – способностью применять методы и средства обеспечения информационной безопасности специальных ИАС;

профессиональными компетенциями:

ПК-10 – способностью осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) **Знать:** -основные положения (основополагающие теоремы) криптологии, вытекающие из теории симметричных и ассиметричных криптографических подходов, а также информационные критерии оценок функционирования криптографических систем (ОПК-7; ПК-10);

2) **Уметь:** - применять эти знания для анализа существующих и вновь проектируемых информационных криптографических систем; - разрабатывать и рассчитывать характеристики криптографической защиты информационных систем в зависимости от назначения этих систем (количество информации, скорость передачи информации, пропускную способность каналов связи, требуемый объём памяти и др.); - при заданных требованиях к техническим характеристикам и показателям качества функционирования систем правильно и аргументированно выбрать (предложить) методы обеспечения этих требований и показателей; - применять современные технологии криптографии в задачах обработки информации (ОПК-7; ПК-10);

3) **Владеть:** -научно-технической терминологией; общими проблемами криптологии, в сфере применения соответствующих задач, возникающих при построении информационных систем различного назначения, а также критерии информационных оценок функционирования этих систем (ОПК-7; ПК-10).

У обучаемых в процессе изучения дисциплины должны вырабатываться дополнительные компетенции, с учетом требований работодателей:

- способность применять основные криптологические алгоритмы для решения прикладных задач в области информационной безопасности.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4 зачетных единицы, 144 часа.

№ п/п	Раздел (тема) дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					Объем учебной работы, с применением интерактивных методов (в часах / %)	Формы текущего контроля успеваемости (по неделям семестра), форма промежуточной аттестации (по семестрам)	
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы,	CPC			
1.	Введение. Основные задачи криптологии. Криптография и криптографический анализ	5	1-2	4	2	4		2	2/20%		
2.	Открытый и закрытый тексты, ключ, основные свойства функции шифрования и дешифрования. Примеры шифров. Шифр Цезаря, Полибия	5	3-4	4	2	4		2	4/40%		
3.	Симметричные шифры. Группы подстановок и перестановок. Чистые шифры. Шифры Виженера и Вернама.	5	5-6	4	2	4		2	2/20%	Рейтинг-контроль №1	
4.	Одноразовый блокнот. Теорема Шеннона об абсолютно стойком шифре. Принцип Керкхоффса. Проблемы симметричной криптографии.	5	7-8	4	2	4		2	4/40%		
5.	Хеш - функции. Хеш - функции, устойчивые в слабом и сильном смысле по отношению к поиску коллизий. Парадокс о днях рождения	5	9-10	4	2	4		2	2/20%		
6.	Блочные Шифры. Стандарты DES, GOST1989. Поточные шифры. Стандарт A5.	5	11-12	4	2	4		2	4/40%	Рейтинг-контроль №2	
7.	Асимметричная криптография. Классы алгоритмической сложности. Сложность математических задач. Односторонние функции	5	13-14	4	2	4		2	4/40%		
8.	Задачи факторизации и дискретного логарифма. Функция Эйлера. RSA. Электронная подпись.	5	15-16	4	2	4		2	4/40%		
9.	Криптографические протоколы. Протокол анонимных вычислений. Схемы разделения секрета. Криптография на эллиптических кривых	5	17-18	4	2	4		2	2/20%	Рейтинг-контроль №3	
Всего				36	18	36		18	KР	28/31%	ЭКЗАМЕН

Содержание разделов дисциплины «Криптографические методы защиты информации»

1. Введение. Симметричная криптография.

Основные задачи теории криптологии. Криптография и криптографический анализ. Краткая справка по истории возникновения и развития, и современному состоянию криптографии.

1.1 Основные понятия криптологии. Открытый и закрытый тексты. Шифры и ключи.

1.2 Канал секретной связи. Возможности противника в канале связи. Определение криптографической системы по Шенону.

1.3 Подстановки и перестановки. Примеры шифров. Шифры Цезаря и Полибия. Двойственность подстановки и перестановки. Теорема о сохранении энтропии открытого текста при применении подстановки и перестановки. Взлом подстановок и перестановок методами частотного анализа закрытого текста.

1.4 Шифр Виженера. Гаммирование. Шифр Вернама и одноразовый блокнот. Теорема Шеннона об абсолютно стойком шифре. Практическая стойкость шифра. Принцип Керкхoffsа.

1.5 Хеш – функции и их свойства. Области применения хеш-функций в криптографии. Необходимые свойства хеш для использования в электронной подписи.

2. Асимметричная криптография. Алгоритмическая сложность.

2.1 Классы алгоритмической сложности. Сложность математических задач. Односторонние функции.

2.2 Задачи факторизации и дискретного логарифма. Функция Эйлера.

2.3 Криптографическая система RSA. Электронные деньги.

3. Криптографические протоколы

3.1 Электронная подпись.

3.2 Протокол Диффи- Хеллмана создания симметричного ключа. МИТМ- атака на протокол.

3.3. Криптографические протоколы. Протокол анонимных вычислений. Схемы разделения секрета. СРС Ади Шамира. Пороговые схемы разделения. Криптография на эллиптических кривых.

4. Криптографический анализ.

4.1 Пассивный криптографический анализ. Частотный анализ.

4.2 Дифференциальный и линейный криптографический анализ. Активный криptoанализ.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Изучение дисциплины предполагает не только запоминание и понимание, но и анализ, синтез, рефлексию, формирует универсальные умения и навыки, являющиеся основой становления специалиста по специальности 10.05.04 «Информационно-аналитические системы безопасности».

Для реализации компетентностного подхода предлагается интегрировать в учебный процесс интерактивные образовательные технологии, включая информационные и коммуникационные технологии (ИКТ), при осуществлении различных видов учебной работы:

- учебную дискуссию;
- электронные средства обучения (слайд-лекции, электронные тренажеры, компьютерные тесты);
- дистанционные (сетевые) технологии.

Как традиционные, так и лекции инновационного характера могут сопровождаться компьютерными слайдами или слайд-лекциями. Основное требование к слайд-лекции – применение динамических эффектов (анимированных объектов), функциональным назначением которых является наглядно-образное представление информации, сложной для понимания и осмысливания студентами, а также интенсификация и диверсификация учебного процесса.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью ОПОП специальности 10.05.04 «Информационно-аналитические системы безопасности», особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом, в учебном процессе, они составляют не менее 30 процентов аудиторных занятий.

Занятия лекционного типа для соответствующих групп студентов согласно требованиям стандарта высшего образования не могут составлять более 55 процентов аудиторных занятий. Программа дисциплины соответствует данным требованиям.

Таким образом, применение интерактивных образовательных технологий придает инновационный характер практически всем видам учебных занятий, включая лекционные. При этом делается акцент на развитие самостоятельного, продуктивного мышления, основанного на диалогических дидактических приемах, субъектной позиции обучающегося в образовательном процессе. Тем самым создаются условия для реализации компетентностного подхода при изучении данной дисциплины.

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Для текущего контроля успеваемости предлагается использование рейтинговой системы оценки, которая носит интегрированный характер и учитывает успешность студента в различных видах учебной деятельности, степень сформированности у студента общекультурных и профессиональных компетенций.

Примерный перечень заданий для текущих контрольных мероприятий:

Вопросы рейтинг-контроля №1:

- Основные задачи криптографии и криptoанализа. Понятие криптообразования. Краткая справка по истории возникновения и развития, и современному криптографии.
- Понятие несимметрии математических операций и трудоемкость элементарных математических операций.
- Понятие криптосистемы.
- Типы криптосистем.
- Криптосистемы с открытым ключом

- Понятие электронной подписи. Необходимость электронной подписи в криптосистемах с открытым ключом.
- Математическая теория групп как основа современных криптосистем.
- Основные математические понятия для конечного поля, характеристика поля.
- Возможность построения конечного поля с необходимым числом элементов.
- Мультиплективная группа конечного поля. Образующие. Дискретный логарифм
- Порядок многочлена над конечным полем.
- Конструкция конечного поля из p^n элементов.
- Псевдослучайные последовательности и их применение в криптографии.
- Алгебра последовательностей над конечным полем.
- Линейные рекуррентные последовательности над конечным полем.

Вопросы рейтинг-контроля №2:

- Конструкция конечного поля из p^n элементов.
- Псевдослучайные последовательности и их применение в криптографии.
- Алгебра последовательностей над конечным полем.
- Линейные рекуррентные последовательности над конечным полем.
- Аннулирующие многочлены.
- Регистр сдвига.
- Экспоненциальный открытый ключ.
- Вычисление дискретного логарифма.
- Число появлений наборов фиксированной длины на полном периоде рекуррентной последовательности.
- Свойства решений линейного рекуррентного уравнения.
- Суммы с характерами.
- Максимальные линейные рекуррентные последовательности как псевдослучайные последовательности.
- Дискретные отображения и признаки хаотичности числовых рядов.

Вопросы рейтинг-контроля №3:

- Аннулирующие многочлены.
- Регистр сдвига.
- Экспоненциальный открытый ключ.
- Вычисление дискретного логарифма.
- Число появлений наборов фиксированной длины на полном периоде рекуррентной последовательности.
- Свойства решений линейного рекуррентного уравнения.
- Суммы с характерами.
- Максимальные линейные рекуррентные последовательности как псевдослучайные последовательности.
- Дискретные отображения и признаки хаотичности числовых рядов.
- Методы криптографии на основе сортировки детерминировано-хаотических рядов.
- Методы криптографии на основе парных сравнений чисел в детерминировано-хаотических числовых рядах.
- Стеганография.
- Оценки и критерии сложности алгоритмов криптографии.
- Криptoанализ и алгоритмические неразрешимые проблемы.
- Особенности хаотических систем.

Перечень вопросов к экзамену (промежуточной аттестации по итогам освоения дисциплины):

1. Основные понятия криптологии: криптография, криptoанализ, шифр, ключ шифра, схема Шеннона секретной связи, симметричные и асимметричные криптосистемы.

2. Группы перестановок и подстановок в криптографии. Двойственность. Теорема о сохранении энтропии для шифров подстановки и перестановки.
3. Определение криптографических систем по Шенону. Примеры шифров по Шенону.
4. Шифр Вижженера (Гаммирование). Взлом Гаммирования.
5. Шифр Вернама. Одноразовый блокнот. Теорема об абсолютно стойком шифре.
6. Классы сложности алгоритмов и задач. Примеры.
7. Односторонние функции. Задачи-кандидаты в односторонние функции.
8. Функции Эйлера и ее свойства. Теорема Эйлера и теорема Ферма.
9. Факторизация целого числа.
10. Дискретный логарифм в конечных полях. Протокол Диффи-Хеллмана.
11. Алгоритм RSA.
12. Электронная подпись в асимметричных схемах и ее свойства. С хеш функциями и без.
13. Хеш функции и их свойства. Криптографические хеш-функции.
14. Криптографические протоколы.
15. Интерполяция многочленами. Теорема о существовании и единственности многочлена. Схема разделения секрета Шамира.
16. Электронные деньги. Неотслеживаемость. Схема Шаума-Педерсана.
17. Стандарты DES и ГОСТ Блочных шифров. Архитектурный и сравнительный анализ шифров.
18. Блочные шифры. Режимы работы блочных шифров.
19. Потоковые шифры.
20. Криптографические модели безопасности. Модель симметричного шифрования, асимметричного и модель Долев-Яо.

Темы практических занятий

- Классы сложности алгоритмов и задач.
- Односторонние функции. Задачи-кандидаты в односторонние функции.
- Функции Эйлера и ее свойства. Теорема Эйлера и теорема Ферма.
- Факторизация целого числа.
- Дискретный логарифм в конечных полях. Протокол Диффи-Хеллмана.
- RSA.
- Электронная подпись в асимметричных схемах и ее свойства. С хеш функциями и без.
- Хеш функции и их свойства. Криптографические хеш-функции.
- Криптографические протоколы.
- Интерполяция многочленами. Теорема о существовании и единственности многочлена. Схема разделения секрета Шамира.
- Электронные деньги. Неотслеживаемость. Схема Шаума-Педерсана.
- Стандарты DES и ГОСТ Блочных шифров. Архитектурный и сравнительный анализ шифров.
- Блочные шифры. Режимы работы блочных шифров.
- Потоковые шифры.

Темы лабораторных работ:

- Лабораторная работа №1. Тема: Шифр Полибия;
- Лабораторная работа №2. Тема: Шифрование файлов. Четыре криптопримитива;
- Лабораторная работа №3. Тема: Многорундовое шифрование;
- Лабораторная работа №4. Тема: Криптографические тесты (NIST).
- Лабораторная работа №5. Тема: Хэш-функция. Электронная подпись;
- Лабораторная работа №6. Тема: Генератор псевдослучайных последовательностей;
- Лабораторная работа №7. Тема: Генерация ключей;

Темы курсовых работ по предмету «Криптографические методы защиты информации».

1. Криптография на эллиптических кривых. Отечественный стандарт электронной подписи.
2. SMT- протоколы передачи информации и их перспективы внедрения.
3. Задача о рюкзаке и рюкзачные криптографические системы. Взлом рюкзаков Меркля.
4. Протоколы доказательства без разглашения. Протокол Фиата – Шамира.
5. Протокол Диффи – Хеллмана создания симметричного ключа. Его слабость по отношению к МИТМ- атаке. Варианты усиления DH – протокола.
6. Стандарт AES (Rijndael), его криptoанализ. Варианты атак на него.
7. Стандарт LTE и его криптографические свойства.
8. Потоковые шифры. Стандарт шифрования A5 и его вариации.
9. Стандарты связи GSM и его защитные модули.
10. Криптография разделения секрета на доли секрета. Визуальная криптография в работе с изображениями.
11. Стеганография.
12. Блочные шифры и различные режимы их работы на примерах DES и GOST1989.
13. Стандарты хеширования. Их криptoанализ. MD5, SHA.
14. Российский стандарт электронной подписи.
15. Электронные деньги. Подпись вслепую электронных купюр Чаума – Педерсена.

Вопросы и задания для самостоятельной работы студентов:

- Какие основные модели цифровых автоматов используются в криптографии?
- Особенности функционирования и взаимодействия цифровых автоматов в криптографических системах.
- Алгоритмы, универсальные алгоритмические системы, достоинства и недостатки;
- Основные понятия и определения, эквивалентность алгоритмов.
- Временная и емкостная сложность алгоритмов.
- Особенности многоядерных процессоров.
- Сопоставительный анализ
- Одномерные и многомерные дискретные отображения, примеры;
- Методы минимизации и их сопоставительный анализ?
- Сложность алгоритмов криптографии. Критерии и оценки;
- Основные соотношения затрат памяти и времени.
- Автоматы на основе дискретного отображения Лоренца, достоинства и недостатки;
- Автоматы на основе отображений TentMap и Хенона, сопоставительный анализ.
- Сопоставительный анализ алгоритмов криptoанализа, оценки сложности;
- Перспективы криptoанализа и алгоритмически неразрешимы проблемы.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Основная литература:

1. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с. ISBN 978-5-369-01378-6, Режим доступа: <http://znanium.com/catalog.php?bookinfo=474838>
2. Кнауб, Л. В. Теоретико-численные методы в криптографии: Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2012. - 160 с. Режим доступа: <http://znanium.com/catalog.php?bookinfo=441493>
3. Карагулова, Н. Г. Защита информации. Курс лекций : Учебное пособие / Н. Г. Карагулова. - Краснодар: КСЭИ, 2014. - 188 с. - Режим доступа: <http://znanium.com/catalog.php?bookinfo=503511>

б) Дополнительная литература:

1. Практическая криптография: алгоритмы и их программирование / Аграновский А.В., Хади Р.А. - М. : СОЛОН-ПРЕСС, 2009. - <http://www.studentlibrary.ru/book/ISBN5980030026.html> 256 с. ISBN 5-98003-002-6.
2. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев - М. : СОЛОН-ПРЕСС, 2009. <http://www.studentlibrary.ru/book/ISBN5980030115.html> 272 с.
3. Башлы, П. Н. Информационная безопасность и защита информации : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2 Режим доступа: <http://znanium.com/catalog.php?bookinfo=405000>

в) Периодические издания:

1. Журнал «Вопросы защиты информации». Режим доступа: http://izumi.ru/editions/detail.php?SECTION_ID=155/
2. Журнал "Information Security/Информационная безопасность". Режим доступа: <http://www.itsec.ru/insec-about.php>.

г) Программное обеспечение и Интернет-ресурсы:

1. Образовательный сервер кафедры ИЗИ.– Режим доступа: <http://edu.izi.vlsu.ru>
2. Информационная образовательная сеть.- Режим доступа: <http://ien.izi.vlsu.ru>
3. Внутривузовские издания ВлГУ.– Режим доступа: <http://e.lib.vlsu.ru/>
4. ИНТУИТ. Национальный открытый университет.– Режим доступа: <http://www.intuit.ru/>

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

ауд. 408-2, Лекционная аудитория, количество студенческих мест – 50, площадь 60 м², оснащение: мультимедийное оборудование (интерактивная доска Hitachi FX-77WD, проектор BenQ MX 503 DLP 2700ANSI XGA), ноутбук Lenovo Idea Pad B5045

ауд. 427а-2, лаборатория сетевых технологий, количество студенческих мест – 14, площадь 36 м², оснащение: компьютерный класс с 8 рабочими станциями Core 2 Duo E8400 с выходом в Internet, 3 маршрутизатора Cisco 2800 Series, 6 маршрутизаторов Cisco 2621, 6 коммутаторов Cisco Catalyst 2960 Series, 3 коммутатора Cisco Catalyst 2950 Series, коммутатор Cisco Catalyst Express 500 Series, проектор BenQ MP 620 P, экран настенный рулонный. Лицензионное программное обеспечение: операционная система Windows 7 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2007, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, программный продукт виртуализации Oracle VM VirtualBox 5.0.4, симулятор сети передачи данных Cisco Packet Tracer 7.0, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 15.0.3.

ауд. 427б-2, УНЦ «Комплексная защита объектов информатизации», количество студенческих мест – 15, площадь 52 м², оснащение: компьютерный класс с 7 рабочими станциями Alliance Optima P4 с выходом в Internet, коммутатор D-Link DGS-1100-16 мультимедийный комплект (проектор Toshiba TLP X200, экран настенный рулонный), прибор ST-031Р «Пиранья-Р» многофункциональный поисковый, прибор «Улан-2» поисковый, вибраакустический генератор шума «Соната АВ 1М», имитатор работы средств нелегального съема информации, работающих по радиоканалу «Шиповник», анализатор спектра «GoodWill GSP-827», индикатор поля «SEL SP-75 Black Hunter», устройство блокирования работы систем мобильной связи «Мозайка-3», устройство защиты телефонных переговоров от прослушивания «Прокрут 2000», диктофон Edic MINI Hunter, локатор «Родник-2К» нелинейный, комплекс проведения акустических и вибраакустических измерений «Спрут мини-А», видеорегистратор цифровой Best DVR-405, генератор Шума «Гном-3», учебно-исследовательский комплекс «Сверхширокополосные беспроводные сенсорные сети» (Nano Xaos), сканирующий приемник «Icom IC-R1500», анализатор сетей Wi-Fi Fluke AirCheck с активной антенной. Лицензионное программное обеспечение: Windows 8 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2010, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, инструмент имитационного моделирования AnyLogic 7.2.0 Personal Learning Edition, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 14.1.4.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности
10.05.04 "Информационно-аналитические системы безопасности", специализация
«автоматизация информационно-аналитической деятельности»

Рабочую программу составил доцент кафедры ИЗИ к.т.н. Александров А.В.
(ФИО, подпись)

Рецензент
(представитель работодателя) Заместитель руководителя РАЦ ООО «ИнфоЦентр»

к.т.н. Вертилевский Н.В.

(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ИЗИ

Протокол № 7 от 28.12.2016 года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/

(ФИО, подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии
по специальности 10.05.04 "Информационно-аналитические системы безопасности",
специализация «автоматизация информационно-аналитической деятельности»

Протокол № ч от 28.12.2016 года

Председатель комиссии д.т.н., профессор

/М.Ю. Монахов/

(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на 2017/2018 учебный год

Протокол заседания кафедры № 1 от 28.08.2017 года

Заведующий кафедрой д.т.н., профессор

/М.Ю. Монахов/

(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой д.т.н., профессор

/М.Ю. Монахов/

(ФИО, подпись)

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)

Институт _____

Кафедра _____

Актуализированная
рабочая программа
рассмотрена и одобрена
на заседании кафедры
протокол № ____ от ____ 20 ____ г.

Заведующий кафедрой

(подпись, ФИО)

Актуализация рабочей программы дисциплины

(наименование дисциплины)

Направление подготовки

Профиль/программа подготовки

Уровень высшего образования

Форма обучения

Владимир 20 ____

Рабочая программа учебной дисциплины актуализирована в части рекомендуемой литературы.

Актуализация выполнена: _____
(подпись, должность, ФИО)

а) основная литература: _____

б) дополнительная литература: _____

в) периодические издания: _____

г) интернет-ресурсы: _____